

AS

4. (Once Amended) The method of claim 1 further comprising the steps of:
determining whether a digital signature key pair update request has been
received from a client unit;
receiving a new digital signature key pair from the client unit in response
to the digital signature key pair update request; and
wherein the step of associating the stored selected expiry data includes
creating a new digital signature certificate containing the selected public key expiry data
selected for the client [generating] that generated the digital signature key pair update
request.

Sub B2

9. (Once Amended) A method for providing updated encryption key pairs in a public
key system comprising the steps of:

A4

providing, through a multi-client manager unit, selectable expiry data
including public key expiry data and selectable private key expiry data that is selectable
on a per client basis;

digitally storing selected public key expiry data for association with a new
encryption key pair; and

associating the stored selected expiry data with the new encryption key
pair to [facilitate] affect a transition from an old encryption key pair to a new encryption
key pair.

10. (Once Amended) The method of claim 9 wherein the step of providing selectable
expiry data includes additionally providing updated digital signature key pairs, the step of
storing includes storing a new digital signature key pair, and the step of associating also
includes associating [the] stored selected expiry data selected for the new digital
signature key pair to [facilitate] affect a transition from an old digital signature key pair
to a new digital signature key pair.

11. (Once Amended) The method of claim 10 wherein the selectable expiry data is
digital signature certificate lifetime data for variably setting a lifetime end date for a

SA cont

~~digital signature certificate [associated with a given client] and [is] also includes encryption certificate lifetime data for variably setting a lifetime end date for an encryption certificate associated with the given client.~~

Selby B3

12. (Once Amended) The method of claim 11 further including the step of providing variable update privilege control on a per client basis to the multi-client manager unit to facilitate denial of updating the digital signature key pair and the encryption key pair.

Selby B3

14. (Once Amended) A system for providing updated digital signature key pairs in a public key system comprising:

Selby B5

multi-client manager means for providing selectable expiry data including at least public key expiry data and selectable private key expiry data that is selectable on a per client basis;

means, accessible by the multi-client manager means, for digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

means, responsive to the stored selected public key expiry data, for associating the stored selected expiry data with the new digital signature key pair to [facilitate] affect a transition from an old digital signature key pair to a new digital signature key pair.

C1

15. (Once Amended) The system of claim 14 wherein the selectable expiry data is digital signature certificate lifetime data for variably setting a lifetime end date for a digital signature certificate [associated with a given client].

16. (Once Amended) The system of claim 14 further including means for providing variable update privilege control on a per client basis to the multi-client manager means to facilitate denial of updating the digital signature key pair on a per client basis.

17. (Once Amended) The system of claim 16 wherein the multi-client manager means includes the means for associating the stored selected expiry data with the new digital

signature key pair and [wherein] includes the means for providing variable update privilege control.

*a 5
cont*

18. (Once Amended) The system of claim 14 further comprising:
means for determining whether a digital signature key pair update request has been received from a client unit;
means for receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and
wherein the means for associating the stored selected expiry data creates a new digital signature certificate containing the selected public key expiry data selected for the client [generating] that generated the digital signature key pair update request.

*B4
B5
A6*

21. (Once Amended) A storage medium comprising:
a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:
allowing entry of selectable expiry data including at least public key expiry data and selectable private key expiry data that is selectable on a per client basis;
digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and
associating the stored selected expiry data with the new digital signature key pair to [facilitate] affect a transition from an old digital signature key pair to a new digital signature key pair.

J1

22. (Once Amended) The storage medium of claim 21 wherein the stored program allows selection of digital signature certificate lifetime data for variably setting a lifetime end date for a digital signature certificate [associated with a given client].

23. (Once Amended) The storage medium of claim 21 wherein the stored program further includes [the facilitating] affecting variable update privilege control on a per